UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/038,169	01/02/2002	Dan Boneh	36321.8009	7811

22918 7590 07/12/2005		EXAMINER
PERKINS COIE LLP		TO, BAO TRAN N
P.O. BOX 2168		
MENLO PARK, CA 94026	ART UNIT	PAPER NUMBER
	2135	

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>02 January 2002</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-28</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-28</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-28 are pending in this application.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1-6 and 8-28 are rejected under 35 U.S.C. 102(e) as being anticipated by

Lewis et al. (U.S. Patent 6,233,565 B1) herein referred to as Lewis.

Regarding on Claims 1 and 28, Lewis discloses a system for protecting sensitive

information residing in server environments, comprising at least one processing device

coupled among at least one network and at least one client computer (col. 2, lines 30-

33), wherein the at least one processing device (server):

receives at least one electronic transaction query (transaction request) from the

at least one client computer (client) via at least one secure channel (SSL) (col. 5, lines

30-40 and col. 15, lines 40-45);

evaluates the at least one electronic transaction query for sensitive data (col. 2,
lines 30-40)

encrypts the sensitive data (col. 14, lines 26-28);

transfers the encrypted sensitive data among components of the server
environment (col. 29, lines 27-34);

receives at least one electronic information query for the encrypted sensitive data
from at least one third-party system via the at least one secure channel (col. 14, lines
25-29);

decrypts the encrypted sensitive data in response to the at least one electronic
information query (col. 16, lines 65-67); and

provides the decrypted sensitive data to the at least one third-party system via
the at least one secure coupling (private network connection) (col. 17, lines 1-5).

Regarding on Claims 2, 26 and 27, Lewis discloses a method for protecting
sensitive information within server environments, comprising:

evaluating at least one electronic request received over at least one secure
Internet channel (SSL) (col. 14, lines 30-40); and

applying at least one cryptographic operation to sensitive data in response to the
at least one electronic request (col. 14, lines 25-28),

wherein sensitive data of the at least one electronic request is encrypted before
transfer among components of the server environment (col. 14, lines 25-30)

wherein encrypted sensitive data of the server environment is decrypted before

transfer from the server environment (col. 17, lines 1-3).

Claims 17 and 25, Lewis discloses a method for securing sensitive information

within server systems, comprising:

evaluating at least one electronic request received from at least one third-party

system via at least one proprietary channel (col. 14, lines 30-40);

determining the at least one electronic request includes a request for encrypted

sensitive data and retrieving the encrypted sensitive data (col. 22, lines 40-50);

decrypting the encrypted sensitive data (col. 16, lines 65-67); and

providing the decrypted sensitive data to the at least one third-party system (col.

17, lines 1-5).

Regarding on Claim 18, Lewis discloses a system for protecting sensitive

information within server systems, comprising

at least one processing device coupled among at least one server site and at

least one client computer and at least one network (FIG. 2, col. 5, lines 30-40 and col.

15, col. 40-45),

wherein the at least one processing device evaluates at least one electronic

request received via the at least one network (col. 2, lines 30-40),

wherein the at least one processing device applies at least one cryptographic

operation to sensitive data in response to the at least one electronic request (col. 14,

lines 25-28),

wherein sensitive data of the at least one electronic request is encrypted prior to

transfer among components of the at least one server system (col. 14, lines 26-28),

wherein encrypted sensitive data of the at least one server system is decrypted

prior to transfer among the at least one network (col. 17, lines 1-3).

Regarding on Claim 3, Lewis discloses the limitations as discussed in Claims 2,

26 and 27 above. Lewis further discloses: comprising determining that the at least one

electronic request includes sensitive data (col. 14, lines 35-40).

Regarding on Claim 4, Lewis discloses the limitations as discussed in Claims 2,

26 and 27 above. Lewis further discloses: wherein evaluating comprises identifying tags

indicating that associated data is sensitive data (col. 37, lines 45-50).

Regarding on Claim 5, Lewis discloses the limitations as discussed in Claims 2,

26 and 27 above. Lewis further discloses: determining that sensitive data in the

electronic request includes at least one user password; and applying at least one hash

function to the at least one user password (col. 22, lines 58-63).

Regarding on Claim 6, Lewis discloses the limitations as discussed in Claims 5 above. Lewis further discloses: wherein the at least one hash function is a keyed hash function or a non-keyed hash function (col. 23, lines 1-10).

Regarding on Claim 8, Lewis discloses the limitations as discussed in Claims 2, 26 and 27 above. Lewis further discloses: wherein the at least one electronic request comprises at least one protocol over Secure Socket Layer (col. 15, col. 40-45).

Regarding on Claims 9 and 21, Lewis discloses the limitations as discussed in Claims 2, 26 and 27 above. Lewis further discloses: wherein the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords (col. 17, lines 5-15).

Regarding on Claim 10, Lewis discloses the limitations as discussed in Claims 2, 26 and 27 above. Lewis further discloses: executing the at least one cryptographic operation using at least one public key (col. 22, lines 20-25).

Regarding on Claims 11 and 22, Lewis discloses the limitations as discussed in Claims 2, 26 and 27 above. Lewis further discloses: wherein the at least one cryptographic operation includes at least one operation selected from a group including

encryption operations, decryption operations, hash operations, keyed hash operations,

and keyed hash verification (col. 22, lines 60-65).

Regarding on Claim 12, Lewis discloses the limitations as discussed in Claims 2,

26 and 27 above. Lewis further discloses: wherein encrypting includes performing at

least one operation on the sensitive data selected from a group including hashing and

keyed hashing when the sensitive data is a password (col. 22, lines 58-64).

Regarding on Claim 13, Lewis discloses the limitations as discussed in Claims 2,

26 and 27 above. Lewis further discloses: wherein the at least one electronic request

comprises at least one encoded key identifier (col. 23, lines 25-35).

Regarding on Claim 14, Lewis discloses a method for securing sensitive

information within server systems, comprising:

parsing at least one electronic request received via at least one Internet coupling

(col. 16, lines 15-25);

determining that the at least one electronic request includes sensitive data (col.

22, lines 40-50);

encrypting the sensitive data (col. 14, lines 26-28); and

storing the encrypted sensitive data in at least one component of the server

system (col. 25, lines 50-60).

Regarding on Claim 15, Lewis discloses the limitations as discussed in Claim 14 above. Lewis further discloses: evaluating at least one request for the encrypted sensitive data (col. 14, lines 25-35),

wherein the at least one request is received via at least one coupling with at least one third-party system (col. 38, lines 15-20);

decrypting the encrypted sensitive data (col. 17, lines 1-3);

providing the decrypted sensitive data to the at least one coupling with at least one third-party system (private network connection) (col. 17, lines 1-5).

Regarding on Claim 16, Lewis discloses the limitations as discussed in Claim 14 above. Lewis further discloses: wherein encrypting includes performing at least one operation on the sensitive data selected from a group including hashing and keyed hashing when the sensitive data is a password (col. 22, lines 58-64).

Regarding on Claim 19, Lewis discloses the limitations as discussed in Claim 18 above. Lewis further discloses: wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags indicating that associated data is the sensitive data (col. 6, lines 1-15).

Regarding on Claim 20, Lewis discloses the limitations as discussed in Claim 18 above. Lewis further discloses: wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags

specified by at least one system administrator that associated data is the sensitive data (col. 6, lines 1-15).

Regarding on Claim 23, Lewis discloses a cryptographic appliance for securing sensitive information within a server system, comprising:

at least one processing device coupled among at least one server system and at least one Internet coupling to evaluate at least one received electronic request (col. 5, lines 30-40 and col. 15, lines 40-45),

wherein the at least one processing device (server) (FIG. 2);

determines when the at least one received electronic request includes sensitive data (col. 22, lines 40-50);

encrypts the sensitive data (col. 14, lines 26-28); and

transfers the encrypted sensitive data among at least one component of the at least one server system (col. 29, lines 27-34).

Regarding on Claim 24, Lewis discloses the limitations as discussed in Claim 23 above. Lewis further discloses: wherein the at least one processing device:

evaluates at least one request for the encrypted sensitive data received via at least one coupling with at least one third-party system (col. 2, lines 30-40);

decrypts the encrypted sensitive data (col. 14, lines 26-28); and

transfers the decrypted sensitive data to the at least one third-party system (col. 17, lines 1-5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis as

applied to claim 2 above, and further in view of Devine et al. (U.S. Patent 6,598,167 B2)

herein referred to as Devine.

Regarding on Claim 7, Lewis discloses the limitations as discussed in Claim 2

above.

Lewis explicitly does not disclose "determining the at least one electronic

request includes at least one cookie; applying at least one cryptographic function or

checksum to the at least one cookie."

However, Devine teaches "determining the at least one electronic request

includes at least one cookie; applying at least one cryptographic function or checksum

to the at least one cookie" (col. 8, lines 45-60).

Therefore, It would have been obvious to one of ordinary skill in the art at the

time the invention was made to incorporate Devine's invention with Lewis to have

included the cookie with the motivation being to allow adding an additional level of

security (col. 8 lines 55-60).

Prior Art

4.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shambroom (U.S. Patent 5,923,756) discloses a method and apparatus is for enhancing the security of a message sent through a network server from a client computer to a destination server. A secure connection for receiving and transmitting data is established between the client computer and the network server. Using client identifying information and a secure authentication protocol, the network server may then obtain client-authentication information form a validation center.

Chang et al. (U.S. Patent 6,105,012) discloses the financial transaction processing system includes at least one financial server connected through a public network to a number of users associated with client computers. Each user accesses the financial server though a web browser. The web browser is provided with the capabilities to generate encryption keys, encrypt and decrypt HTML forms, and to digitally sigh and timestamp HTML forms.   The financial server transfers web pages including HTML forms representing financial transactions.

Contact Information

5.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bao Tran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Bao Tran N. To
Patent Examiner
07/07/2005
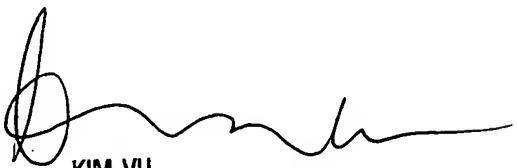
KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100